EXHIBIT 16

ISS'S STATEMENT OF ANTICIPATED PROOFS

ISS expects that it will offer the following proof at trial, subject to revision based upon the Court's rulings on any pending motions, or in response to new matters introduced in SRI's Statement of Anticipated Proofs. In addition to the items identified below, ISS intends to prove the matters identified in its Answer and Counterclaims to SRI's First Amended Complaint, interrogatory answers, and in the expert reports of its expert witnesses. ISS also intends to offer proof on the issues of fact and issues of law identified by the parties in this Joint Pretrial Order.

For the Court's convenience, SRI has asserted the following claims against ISS (referred to herein as the "asserted ISS claims"):

Asserted ISS claims	'338 patent: claims 1, 4, 5, 11, 12, 13, and 24 '203 patent: claims 1, 2, 4, 6, 12, 13, 15, and 17 '615 patent: claims 1, 2, 4, 13, 14, and 16

I.   INVALIDITY OF THE PATENTS-IN-SUIT

ISS will introduce proof that:

1.   The asserted ISS claims of the '338, '203, and '615 patents are invalid under 35 U.S.C. § 102(a), (b), and (e) as anticipated, based upon the following prior art publications and systems or products:

- P. Porras and A. Valdes, "Live Traffic Analysis of TCP/IP Gateways," ("*Live Traffic*" various versions);

- P. Porras and P. Neumann, "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," Proceedings of the 20th National Information Systems Security Conference, pp. 353-365, October 9, 1997 ("*Emerald 1997*");[1]

- D. Anderson, T. Frivold, and A. Valdes, "Next-generation Intrusion Detection Expert System (NIDES) A Summary," Computer Science Laboratory, SRI-CSL-

---

[1] The Court previously determined that EMERALD 1997 is a prior art printed publication under 102(b).

95-07, May 1995 ("*Network NIDES*");

- Y. Frank Jou et al., "Architecture Design of a Scalable Intrusion Detection System for the Emerging Network Infrastructure," Technical Report CDRL A005, Dept. of Computer Science, North Carolina State University, April 1997 ("*JiNao Report*");

- L. Todd Heberlein et al., "A Network Security Monitor," Proc. 1990 IEEE Computer Society Symposium on Research in Security and Privacy, pp. 296-304, May 1990 ("*NSM 1990*");

- L.T. Heberlein, B. Mukherjee, K.N. Levitt, "Internetwork Security Monitor," Proc. of the 15th National Computer Security Conference, pp. 262-271, October 1992 ("*ISM 1992*");

- B. Mukherjee, L.T. Heberlein, K.N. Levitt, "Network Intrusion Detection," IEEE Network, Vol. 8 No. 3, pp. 26-41, June 1994 ("*NID 1994*");

- Steven R. Snapp et al., "Intrusion Detection Systems (IDS): A Survey of Existing Systems and a Proposed Distributed IDS Architecture," CSE-91-7, Feb. 1991 ("*DIDS Feb. 1991*");

- Steven R. Snapp et al., "DIDS (Distributed Intrusion Detection System) – Motivation, Architecture, and An Early Prototype," Proc. 14th National Computer Security Conference, pp. 167-173, October 1991 ("*DIDS Oct. 1991*");

- S. Staniford-Chen et al., "GrIDS – A Graph Based Intrusion Detection System for Large Networks," 19th National Information Systems Security Conference, pp. 361-370, October 1996 ("*GrIDS 1996*");

- Steven Cheung et al., "The Design of GRIDS: A Graph-Based Intrusion Detection System," Technical Report, UC Davis Department of Computer Science, Davis California, May 14, 1997 ("*GrIDS 1997*");

- "NetStalker, Installation and User's Guide, Version 1.0.2" (May 1996);

- "RealSecure Release 1.0 for Windows NT 4.0 A User's Guide and Reference Manual";

- "NetRanger User's Guide Version 1.3.1," WheelGroup Corporation, 1997 ("*NetRanger Manual*");[2]

- Network Security Monitor ("NSM");

- Distributed Intrusion Detection System ("DIDS");

- Graph-based Intrusion Detection System ("GrIDS");

- NetRanger;

- ISS RealSecure; and

---

[2] SRI has stipulated this is a 102(b) prior art reference.

2

- NetStalker.

2.   The asserted ISS claims of the '338, '203, and '615 patents are invalid under 35

U.S.C. § 103 as obvious based upon the combination of two or more of the following references:

- All prior art publications and systems or products listed in (1) above;

- L.T. Heberlein, B. Mukherjee, K.N. Levitt, "A Method to Detect Intrusive

  Activity in a Networked Environment," Proc. 14th National Computer Security

  Conference, pp. 362-371, Oct. 1991;

- H.S. Javitz and A. Valdes, "The NIDES Statistical Component Description and

  Justification," Annual Report A010, March 1994;

- A. Valdes and D. Anderson, "Statistical Methods for Computer Usage Anomaly

  Detection using NIDES," Proc. of the Third International Workshop on Rough

  Sets and Soft Computing, January 1995;

- SunScreen EFS Configuration and Management Guide, Release 1.1, Rev. A,

  Sun Microsystems, June 1997;

- CERT Advisory CA-1996-21 TCP Syn Flooding and IP Spoofing Attacks;

- CERT Advisory CA-1996-26 "Denial-of-Service Attack via Ping, Dec. 18,

  1996; and

- Any additional obviousness references relied upon in the Defendants' expert

  reports, including but not limited to additional references regarding the Network

  Security Monitor, the Distributed Intrusion Detection System, the Graph Based

  Intrusion Detection System, the ISS RealSecure system, the NetStalker system,

  and the NetRanger system.

3.   The asserted ISS claims of the '338, '203, and '615 patents are invalid under 35

U.S.C. § 112 for failure to satisfy the best mode requirement.

4.   The asserted ISS claims of the '203 and '615 patents are invalid under 35 U.S.C. § 112 for failure to satisfy the written description requirement.

5.   Rebuts SRI's assertions of the existence of evidence of secondary indicia of nonobviousness, and any evidence of a purported nexus between alleged secondary indicia and the purported invention(s) of the '338, '203, and '615 patents.

6.   Objective evidence of obviousness that supports a finding that the asserted claims were obvious over the prior art.

II.   UNENFORCEABILITY OF THE PATENTS-IN-SUIT

ISS will introduce proof that:

7.   Individuals associated with the filing or prosecution of the '338, '203, and '615 patents either withheld information from the United States Patent & Trademark Office (the "PTO") or misrepresented information to the PTO.

8.   The information withheld or misrepresented by individuals associated with the filing or prosecution of the '338, '203, and '615 patents was material.

9.   The information withheld or misrepresented by individuals associated with the filing or prosecution of the '338, '203, and '615 patents was withheld or misrepresented with the intent to mislead or deceive the PTO.

III.   NONINFRINGEMENT

ISS will introduce proof that:

10.   Rebuts SRI's assertion that ISS's operation of the RealSecure agents (Network, Guard, Server, and Desktop series) and Proventia agents (A, G, M, Server and Desktop series) ("the ISS sensors") when used in combination with the SiteProtector SecurityFusion Module 2.0

(as well as later versions) meets each and every limitation of the asserted ISS claims of the '203 and '615 patents, either literally or with only insubstantial differences.

11.   Rebuts SRI's assertion that ISS or any ISS customer has directly infringed the asserted ISS claims of the '203 and the '615 patents in the manner alleged to be infringing.

12.   Rebuts SRI's assertion that ISS, with the requisite intent and knowledge, actively induced its customers to operate the ISS sensors in combination with the SiteProtector SecurityFusion Module 2.0 (as well as later versions) to infringe the asserted ISS claims of the '203 and '615 patents.[3]

13.   Rebuts SRI's assertion that ISS's use or sale of the Proventia Network Anomaly Detection System (ADS) product operating in standalone mode meets each and every limitation of the asserted ISS claims of the '338 patent, either literally or with only insubstantial differences.

14.   Rebuts SRI's assertion that ISS or any ISS customer has directly infringed the asserted ISS claims of the '338 patent in the manner alleged to be infringing.

15.   Rebuts SRI's assertion that ISS, with the requisite intent and knowledge, actively induced its customers to use the Proventia Network Anomaly Detection System (ADS) product operating in standalone mode to infringe the asserted ISS claims of the '338 patent.

---

[3] ISS understands that SRI is no longer asserting contributory infringement against any ISS product.